# Bezpieczeństwo systemów i sieci

Marcin Szewczyk <Marcin.Szewczyk@wodny.org>

25 maja 2009

# 1 Wstęp

W tym artykule chciałbym Czytelnikowi pokrótce przedstawić mój punkt widzenia na współcześnie zagrażające mu ataki pochodzące z sieci lub bezpośrednio z samodzielnie zgromadzonych nośników. Czyli...

## 1.1 Co konkretnie

...skupię się na tym, kto i przy użyciu czego atakuje nasze komputery. Opiszę, jak można się bronić. W artykule znajdują się fakty uważane przez bardziej doświadczonych użytkowników za oczywiste, ale warto o nich wspomnieć dla jasności rozważań. Wspomniałem również o kilku, mam nadzieję, mniej znanych zjawiskach.

# 2 Zagrożenia ogólnie

Użytkownik narażony jest na utratę danych lub, co być może gorsze, na ujawnienie tych poufnych. Wiązać się to może z prostym socjologicznie podpartym dyskomfortem lub utratą pieniędzy. Na komputerze trzymamy hasła, historię rozmów, emaile, numery kont, archiwalne nagrania audio i video, projekty i wiele innych rzeczy. To wszystko może pewnego dnia zniknąć lub zostać umieszczone w sieci.

Zagrożeniem, choć istotnym głównie dla dostawców usługi, jest również odcięcie od usługi – *Denial of Service*.

# 3 Zagrożenia od strony technicznej

## 3.1 Malware

Ogólnie złośliwe oprogramowanie można określić mianem *malware*[2]. W tej rodzinie mieszczą się wirusy niszczące dane, konie trojańskie wykradające dane, *rootkity* i wszelkie ich hybrydy. Dawno temu wirusy lubiły dane kasować. Współcześnie dużo częściej je wykradają. Informacja jest po prostu wiele warta, również dosłownie - nic tak nie cieszy jak zestaw haseł prowadzących do pieniędzy na kontach bankowych.

Przy okazji warto wspomnieć, że współcześnie popularne są zagrożenia, które nie wymagają by uruchomić je dwuklikiem, aby mogły przejąć kontrolę. Powszechnie występują tzw. *exploity*[3]. Są to specjalnie przygotowane dane, często w formie dokumentu tekstowego, graficznego czy utworu muzycznego, które po otwarciu w konkretnej aplikacji wykorzystują błędy jej twórców-programistów. Przeprowadzenie takich ataków jest tym prostsze, że istnieją projekty pokroju *Metasploit*[4] – klikalne i proste w obsłudze.

## 3.2 Wygoda

Powszechnie wiadomo, że wygoda jest wrogiem bezpieczeństwa. 100% pewności nie uzyskamy nigdy. Należy określić swój własny satysfakcjonujący poziom bezpieczeństwa. W tej sekcji jako przykład może posłużyć funkcja *autouruchamiania*[1] dostępna w Windows – przez pierwsze 5 min. miła zabawka zwiększająca ergonomię, na co dzień jedna ze skuteczniejszych metod roznoszenia wirusów.

## 3.3 Naiwność

Nie zawsze jest tak, że jesteśmy bezbronni, ponieważ mamy dziurawy system i możemy tylko czekać, aż ktoś go przejmie, byśmy ostatecznie mogli zakończyć tydzień formatowaniem dysku. Wiele zagrożeń wymaga od użytkownika interakcji i żeruje na jego naiwności.

## 3.4 Euforia

Dość często spotykanym zjawiskiem jest przekonanie zabezpieczającego o jego geniuszu. Niestety brak empirycznego testu, czy użyte środki przyniosły pożądany efekt, źle wróży. Poza tym trzeba pamiętać, by efekty swej pracy zachować w pamięci trwałej tak, by obowiązywały również przy następnym uruchomieniu komputera.

# 4 Dobre praktyki

Dlatego właśnie przestawię teraz skomponowane wg własnego uznania *dobre praktyki*.

## 4.1 Wymyślanie koła

Nie należy wymyślać koła jeszcze raz. Wiele problemów zostało już dobrze zdefiniowanych. Części z nich towarzyszą dobrze zdefiniowane rozwiązania.

Warto przeczytać opinie innych. Jeszcze lepiej jeśli są to opinie osób poważanych. Znakomicie, jeśli są to opublikowane przez znane osoby opinie zebrane w standard i oddane na pastwę komentarzy technicznej części społeczności internetowej. Ta uwaga dotyczy szczególnie zagadnień związanych z kryptografią.

## 4.2 Z wielką siłą wiąże się wielka odpowiedzialność

Ten wyświechtany cytat miał mi posłużyć do tego, by wspomnieć o jednym z większych zagrożeń czyhających na użytkowników Windows w domyślnej konfiguracji. Otóż podstawowe konto ma uprawnienia administratora. W ten sposób uruchomione przez nas złośliwe oprogramowanie również zyskuje prawa administratora. Tym samym tracimy możliwość wyczyszczenia komputera inaczej niż przez odpalenie innego systemu operacyjnego. Na koncie bez uprawnień administratora da się pracować. Gdy jeszcze korzystałem z Windows, jedyną aplikacją, która się nie poddała, była gra CounterStrike.

## 4.3 Małpa w kąpieli

Zdarza się, że podczas odwiedzin jakiejś strony przeglądarka ostrzega nas o wadliwym certyfikacie SSL. Nie należy takiego certyfikatu akceptować, jeśli odwiedzamy stronę, na której wcześniej takie problemy nie występowały, a w ogólności, jeśli mamy jej podać jakieś poufne informacje. Prawdą jest, że małe instytucje stosują samopodpisane certyfikaty wyłącznie do szyfrowania (wtedy możemy się dowiedzieć innym kanałem od administratora, czy *odcisk palca* certyfikatu jest zgodny), ale znaczące instytucje pokroju banków nie dopuszczają do takich sytuacji.

## 4.4 Listonosz zawsze puka dwa razy

Podobnie jak nie bierzemy udziału w łańcuszkach, piramidach finansowych i nie kupujemy zestawu niezawodnych śrubokrętów na każdą okazję na podstawie przesyłki znalezionej w tradycyjnej skrzynce na listy, tak nie powinniśmy obdarzać zaufaniem tego, co znajdziemy w skrzynce elektronicznej. Poczta elektroniczna odziedziczyła kilka cech po poczcie tradycyjnej. Po pierwsze adres nadawcy wyświetlany przez program nie musi być prawdziwy[6][5]. Po drugie, jeśli ktoś znienacka chce pomóc w załataniu systemu lub wykasowaniu wirusa – bądź czujny. Jeśli w mailu otrzymałeś "łatę" a nadawcą jest Microsoft – na pewno jest to wirus. Po trzecie złośliwy użytkownik (analog złośliwego sąsiada) może czyjąś pocztę przechwycić, przeczytać i zmodyfikować przed jej dotarciem do celu. W tym miejscu można przejść do krótkiej instrukcji – jak zostać asem wywiadu.

## 4.5 Karmienie paranoi

Współcześnie dysponujemy technikami, które zapewniają nas, że czytana treść pochodzi rzeczywiście od osoby, której podpis widzimy, a wszystko możemy jeszcze zaszyfrować, by wścibski sąsiad nie ukradł nam sekretnego przepisu kulinarnego. Co więcej, by korzystać z tych udogodnień, nie musimy być specjalistami w zakresie kryptografii. Dla użytkowników Windows jest PGP, dla ornitologów - GnuPG. Aplikacje są ze sobą z grubsza kompatybilne, a zyskujemy dzięki nim chociażby możliwość dołożenia do swej korespondencji wyżej wymienionych cech.

Możemy pójść jeszcze dalej i zaszyfrować dane na dysku – w ten sposób w przypadku kradzieży nośnika nie musimy się martwić, że dane wyciekną. Wśród moich znajomych korzystających z Windows popularny jest program *TrueCrypt*. Sam na Linuksie stosuję *cryptsetup* z dodatkiem *LUKS*. Istotny jest jednak pewien szczegół. Jeśli nie szyfrujemy wszystkich dysków, musimy mieć na uwadze, że system operacyjny może ujawniać dane w plikach tymczasowych oraz w obszarze *swap* (pliku wymiany). Dlatego, jeśli zaszyfrowaliśmy wybiórczo tylko nasze przepisy kulinarne, zaszyfrujmy również dwie powyższe lokalizacje.

## 4.6 Kiepska administracja sieci

Może się zdarzyć również tak, że administratorzy sieci nie potrafią lub nie mogą zabezpieczyć klientów przed niektórymi atakami. Najczęściej uprzykrzyć życie użytkownikom sieci można poprzez uruchomienie konkurencyjnego serwera *DHCP* oraz podszywanie się pod bramę domyślną[7]. Choć nie jest to rozwiązanie eleganckie, w takiej sytuacji można po prostu skonfigurować adresy IP: swój, bramy domyślnej i *DNSów* – statycznie. Do tego

należy jeszcze utworzyć statyczne wpisy w tablicy *adresów MAC / ARP*.

### 4.7 Dbaj o swój system

Każdy system operacyjny wymaga aktualizacji. W Windows o konieczności aktualizacji plików systemowych poinformuje użytkownika żółta tarcza przy zegarze. O konieczności aktualizacji poszczególnych aplikacji czasem informują one same.

Dla użytkowników Linuksa przydatne mogą się okazać applety dostarczane wraz ze środowiskami graficznymi pokroju *Gnome* lub niezależny od nich zestaw narzędzi *apt-get*, *aptitude* oraz *apticron*.

Zawsze warto czytać biuletyny informacyjne, grupy dyskusyjne, wydania elektroniczne magazynów dotyczących tematyki bezpieczeństwa[8].

Przy okazji warto zaznaczyć, że np. biuletyny z informacjami o łatach od Microsoftu przychodzą popisane przy pomocy *SHA-256* i *RSA*[9].

### 4.8 Połączenia bezprzewodowe

Jeśli łączysz się z siecią bezprzewodową, to nigdy nie wybieraj otwartej nieszyfrowanej sieci. Nie podłączaj się również do sieci szyfrowanej wg protokołu *WEP* – do takiej sieci można się włamać w kilka minut[10].

Współcześnie bezpieczne standardy to *WPA* i *WPA2* oraz ich wersje *Enterprise*.

### 4.9 Przepis na hasło

Dość poważnym problemem zabezpieczania zasobów jest tajny klucz, którym będziemy je chronić. Współcześnie uwierzytelnianie metodami biometrycznymi w kontekście komputerów osobistych nadal raczkuje. Dlatego najpopularniejszym sposobem ochrony jest hasło. Warto wybrać takie, którego atakujący nie domyśli się w krótkim czasie. Niech nie będzie jednym, czy sklejeniem dwu lub trzech wyrazów ze słownika. Powinno zawierać małe i duże litery, cyfry oraz znaki specjalne jak %, # itp. Siłę swojego hasła można sprawdzić dostępnymi w Internecie narzędziami[11], ale używać należy tylko tych, co do których mamy pewność, że przy okazji ich nie wykradną.

I jeszcze trzy ważne kwestie. Po pierwsze, hasło nie może być dołączone do obiektu, który chroni. Nie piszmy więc kodu PIN na karcie płatniczej. Po drugie – nie używaj tego samego hasła wszędzie. Po trzecie, każdy komputer, którym nie opiekujesz się osobiście, jest potencjalnie maszyną wykradającą hasła.

### 4.10 Zapewnienie zapasowej łączności

Współcześnie dysponujemy często telefonem stacjonarnym, komórkowym i osobnym łączem internetowym. Wszystkie te usługi są mocno powiązane. Łączność z Internetem można przecież uzyskać wdzwaniając się modemem przez zwykłe łącze telefoniczne (tak jak czyniło się to drzewiej). Można nawiązać analogiczne połączenie dzięki technologii GPRS lub UMTS podłączając do komputera telefon komórkowy.

W ramach samego połączenia z Internetem można również zapewnić sobie nadmiarowość kanałów komunikacyjnych. Można założyć kilka kont pocztowych u kilku dostawców. Istotny może również okazać się wybór technologii *instant messaging*. W Polsce popularne jest GaduGadu. Osobiście jednak kilka miesięcy temu zrezygnowałem ostatecznie z tego rozwiązania. Używam od paru lat technologii Jabber[12] [13]. U jej podstaw leży założenie, iż użytkownicy zakładają konta u wielu dostawców. Dostawcy ci natomiast przesyłają wiadomości między sobą.

Dzięki powyższym rozwiązaniom nawet w sytuacji awaryjnej możemy utrzymać przepływ informacji.

## 5 Aktywna obrona

### 5.1 Antywirus a firewall

Niestety pojęcia *program antywirusowy* i *firewall* są często mylone przez użytkowników. Warto zaznaczyć, że są to narzędzia zdecydowanie różne - różnie działające i mające różne zadania. Prawdą jest natomiast, że na rynku istnieją produkty łączące mniej lub bardziej udanie obie funkcjonalności (np. Avast). Ja wolę jednak aplikacje o dobrze zdefiniowanych funkcjach.

### 5.2 Antywirus zatem

Program antywirusowy ma wykrywać zagrożenia gnieżdżące się w przeglądanych i uruchamianych

plikach oraz ewentualnie w odbywających się transmisjach sieciowych. Detekcja odbywa się po pierwsze na podstawie porównania powyżej wymienionych danych z sygnaturami z bazy – czyli fragmentami kodu wykonywalnego wirusów. Po drugie na podstawie detekcji kodu charakterystycznego dla wrogich działań - np. takiego, który próbuje zmodyfikować *MBR*.

Jeszcze, gdy Windows był moim podstawowym system operacyjnym, korzystałem z AVG jako programu antywirusowego. Potrafił skanować na żądanie, miał filtr rezydenty, w ostateczności można było skorzystać z filtra poczty. Przede wszystkim był jednak darmowy. Czytelnikowi sugeruję właśnie to kryterium wyboru. Dobre praktyki są dużo ważniejsze od złudnego poczucia bezpieczeństwa, które dają kobyłki antywirusowe, za które trzeba słono zapłacić. Nawet najlepszy zestaw sygnatur i heurystyka nie dają zadowalającego poziomu bezpieczeństwa. Mieszkając w akademiku uzyskałem potwierdzenie tej teorii – systemy ewidentnie zawirusowane (co stwierdziliśmy na podstawie ich zachowania w sieci) wg popularnego programu antywirusowego wyposażonego we wszystkie aktualizacje były czyste.

Na Linuksie programu antywirusowego nie stosuję. Nie dlatego, że uważam, iż nie istnieją wirusy na ten system – bo to nieprawda. Sposób pracy jest inny, od początku nabiera się innych przyzwyczajeń. Poza tym większość oprogramowania pochodzi z repozytorium dystrybucji.

## 5.3 Firewall

Firewall zwany po polsku zaporą ogniową to filtr pakietów, które przepływają przez naszą maszynę. Chroni nas przed atakami czysto sieciowymi (np. próbą zalania naszego komputera ogromną ilością pakietów) czy przed atakami na konkretne aplikacje.

Na Linuksie firewalle buduje się aktualnie przy pomocy *iptables*[14]. Jądro tego systemu wraz ze wszystkimi modułami jest niezwykle bogatym narzędziem. Warto przeczytać jego dokumentację.

Na systemie Windows przez wiele lat używałem jako zapory programu Sunbelt Kerio Personal Firewall. Świetne narzędzie, bogate w opcje. Co więcej jest darmowe do użytku prywatnego (po 30 dniach wyłącza się kilka funkcji, ale są to w zasadzie wodotryski). Ma również wbudowany IDS (System Detekcji Włamań), czyli moduł wykrywający zagrożenia na podstawie wzorców zachowań. W przypadku Linuksa IDS uruchamia się raczej na maszynach, które pomagają zarządzać siecią, rzadziej na osobistym komputerze[15].

Praktycznie rzecz biorąc *iptables* na osobistym komputerze niezbędne nie jest. W tej chwili na moim komputerze nie nasłuchuje na żadnym porcie żadna usługa. Na systemie Windows firewall jest niezbędny. Tutaj wiele usług czeka na przychodzące połączenia. Biorąc pod uwagę, iż w usługach są dziury[16], uruchamiają się one na prawach konta SYSTEM (czyli najwyższych), a na łaty trzeba czekać długo, wystawiamy się na niebezpieczeństwo. I znów – z praktycznego punktu widzenia, komputer osobisty nie powinien mieć potrzeby nasłuchiwać na połączenia z wyjątkiem sytuacji, gdy np. udostępnia pliki po protokole FTP - wtedy jednak warto zezwolić na połączenia przychodzące jedynie na wybrane porty.

Na koniec warto jeszcze wspomnieć, że *NAT* a firewall to dwie różne rzeczy. *NAT* sam w sobie bezpieczeństwa nie wnosi – będzie pozwalał na ataki na komputery wewnątrz sieci maszynom oddalonym o jeden hop na zewnątrz sieci, ponieważ w głębi jest również routerem.

## 5.4 Poprawienie bezpieczeństwa poszczególnych aplikacji

### Eksplorator Windows

Wyłącz ukrywanie rozszerzeń, ta opcja potrafi zgubić, gdy wirus ma ikonkę np. dokumentu tekstowego. Wyłącz autouruchamianie[1].

### Firefox

Jeśli jest się gotowym poświęcić chwilę na dostosowanie reguł, to warto do Firefoksa doinstalować dodatki (rozszerzenia) NoScript i AdBlock Plus – mogą pracować jednocześnie. Wspólnie uchronią nas przed samoistnym uruchamianiem się aplikacji Flash, skryptów JavaScript czy otwieraniem się PDFów. Dla stron zaufanych można błyskawicznie dodać wyjątki, na reszcie stron warto mieć wyłączone powyższe funkcjonalności. Każdy kolejny moduł w aplikacji to kolejne zagrożenia. Gdy piszę ten artykuł na wolności grasuje *exploit*, dzięki któremu można przejąć kontrolę nad kontem użytkownika

zmuszając go jedynie do wejścia na stronę z obsadzonym dokumentem PDF[3].

#### Opera

W przeglądarce Opera da się uzyskać podobny efekt przy pomocy wbudowanych opcji globalnego wyłączania wtyczek i JavaScript oraz dodanie wyjątków dla stron zaufanych.

### 5.5 Podsumowanie

Mam nadzieję, że ta garść porad okaże się przydatna i życzę Czytelnikowi aseptycznego roku.

## Literatura


[1] How to disable the Autorun functionality in Windows, Microsoft Help and Support, http://support.microsoft.com/kb/967715

[2] Symantec about malware, http://www.symantec.com/norton/security_response/malware.jsp

[3] Secunia, Adobe Reader/Acrobat Multiple Vulnerabilities, http://secunia.com/advisories/33901/

[4] The Metasploit Project, http://www.metasploit.com/

[5] RFC-2822, 3.6.2. Originator fields, http://tools.ietf.org/html/rfc2822#section-3.6.2

[6] RFC-2821, 7.1 Mail Security and Spoofing, http://tools.ietf.org/html/rfc2821#section-7.1

[7] ARP Spoofing, http://en.wikipedia.org/wiki/ARP_spoofing

[8] Bugtraq (bugtraq) Mailing List, http://seclists.org/rss/bugtraq.rss

[9] Microsoft Security Response Center PGP Key and S/MIME Certificate, https://www.microsoft.com/technet/security/bulletin/pgp.mspx

[10] Aircrack-ng, http://aircrack-ng.org/

[11] Microsoft Password checker, http://www.microsoft.com/protect/yourself/password/checker.mspx

[12] XMPP Technologies: Overview, http://xmpp.org/tech/overview.shtml

[13] Jabber vs GaduGadu, opracowanie własne, http://wodny.org/permalink/92/Jabber_vs_GaduGadu.html

[14] The netfilter.org project, http://www.netfilter.org/

[15] How To Guide: Intrusion Detection Systems, Brian Laing, ISS, http://www.snort.org/docs/iss-placement.pdf

[16] Secunia, Vulnerability Report: Microsoft Windows Vista, http://secunia.com/advisories/product/13223/?task=advisories